IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF NORTH CAROLINA
ASHEVILLE DIVISION

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FACEBOOK ACCOUNTS:<br><br>Andrew DeVinney WITH ASSOCIATED USER ID 100010733371225, and<br><br>John Smith WITH ASSOCIATED USER ID 100052453491283<br><br>THAT IS STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC. | Case No. 1:24-mj-00038-WCM<br><br>**Filed Under Seal** |

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Jared Schaefer, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application for a search warrant for information associated with a certain Facebook account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), a company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Meta to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the accounts.

2. I am a Special Agent with the Federal Bureau of Investigation Charlotte Division / Hickory RA and have been since October 2023. My career in law enforcement began in May of 2020, where I spent three years as a sworn Police Officer/Detective with the La Porte Police

Department (LPPD) in Indiana. I spent approximately the first year tasked with completing the police academy, performing road patrol duties which consisted of responding to 911 calls for police assistance for all types of crimes, conducting self-initiated activities to deter crime, taking part in community engagement initiatives and numerous other jobs vital to LPPD's mission; being a member of the Detective Bureau where I conducted a number of logical investigations into robberies, burglaries, sexual assaults, child molestations, murder, and other violent crimes for approximately two years. In my time as a law enforcement officer, I have received several hundred hours of training in the investigations of general crimes, and I have been directly or indirectly involved with investigations of cases of child sexual assault. I have participated in the execution of numerous search warrants, which have resulted in the seizure of evidence and the successful prosecution of individuals.

3. For the purpose of supporting this Application for a Search Warrant, I have set forth herein facts that I believe are sufficient to establish probable cause to believe that evidence of violations of 18 U.S.C. § 2252A(a)(2)(A) (receipt and distribution of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of, knowing access, or attempted access with intent to view child pornography) by Andrew C. DEVINNEY will be found in the Meta account(s) described below:

- Andrew DeVinney with associated user ID 100010733371225; and
- John Smith with associated user ID 100052453491283.

This Affidavit refers to the above Meta accounts collectively as the "TARGET ACCOUNTS." The TARGET ACCOUNTS are further described in Attachment A. The TARGET ACCOUNTS are stored at premises owned, maintained, controlled, or operated by Meta. The applied-for warrant would order Meta to provide information described in Attachment B.

4. The information in this Affidavit is based upon my personal knowledge, training, and experience, and information learned, either directly or indirectly, from witnesses, records, and other law enforcement officers and agents. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

## PROBABLE CAUSE

5. On August 5, 2024, the Burke County Sheriff's Office (BCSO) received three CyberTips from the National Center for Missing and Exploited Children (NCMEC) regarding the distribution and receipt of child pornography between Andrew C. DEVINNEY and Starla Stamey. Two of the three CyberTips documented distributions of child pornography via Facebook Messenger. NCMEC's CyberTipline reporting system allows electronic service providers, like Facebook, to make reports of suspected online sexual exploitation of children, including the distribution and receipt of child pornography, occurring on their platforms.[1]

### *CyberTip 1*

6. NCMEC received CyberTip #194669154 (CyberTip 1) from Facebook on June 4, 2024, at approximately 10:20PM (UTC). This tip identified DEVINNEY as sending files depicting child pornography to an individual named Starla Stamey via Facebook Messenger.

7. CyberTip 1 identified a total of three files that DEVINNEY sent to Stamey on May 30, 2024, at approximately 2:09PM (UTC), using Facebook Messenger username "Andrew DeVinney" (screenname: andrew.devinney.3). Facebook identified one of the three files sent by

[1] "Overview," National Center for Missing & Exploited Children CyberTipline, https://www.missingkids.org/gethelpnow/cybertipline.

DEVINNEY as depicting child pornography by running the file's unique MD5 hash value[2] against hash values for known series of child pornography and confirmed that the file did in fact match a previously identified video of child pornography. The identified file depicted a one minute and fifty-four second video of an adult white male forcing vaginal sex on a 6- to 8-year-old prepubescent female.

8. According to Facebook records, the "Andrew DeVinney" Facebook account was associated with phone numbers 828-302-9582 and 828-403-4141. The email address associated with the "Andrew DeVinney" Facebook account was andrewdevinney94@gmail.com. DEVINNEY's Facebook account used IP address 75.143.188.107, which was provided by Spectrum/Charter to a location in Morganton, North Carolina.

9. According to Facebook records, Stamey's Facebook Messenger account used the screen name "Starla.stamey.3" and was associated with phone number 828-409-4061. CyberTip 1 reported that Stamey's birth date was July 23, 1995, and that Stamey's account was used in Morganton, North Carolina. Stamey's listed verified phone number was 828-409-4061. The IP address listed for Stamey's account was 149.168.240.6, which resolved to a Virtual Private Network (VPN)[3] server in the Raleigh, North Carolina area.

---

[2] A hash value is a unique numeric value that is assigned to a digital file by processing it through a cryptographic algorithm. MD5 is a commonly used cryptographic algorithm to generate hash values. This number, the hash value, becomes a unique identifier for the file. Any change to the digital file likewise will change the hash value. Hash values are often analogized to a DNA profile. The probability of two different digital files sharing the same hash value is nearly impossible, so if two files have the same hash value then one may safely assume that the files are identical.

[3] Your Affiant knows that a VPN is a computer-based service that encrypts data and masks IP addresses to create a secure connection between a device and a remote server. A VPN user may be connected to a server in Raleigh, North Carolina without being in the vicinity of Raleigh.

10. NCMEC performed a public records search of the phone numbers from CyberTip 1. Phone number 828-403-4141 belongs to an AT&T Mobility account held by DEVINNEY at 3695 Ridge Ct., Morganton, North Carolina 28655. Phone number 828-302-9582 belongs to a T-Mobile account held by Stamey, also at 3695 Ridge Ct., Morganton, North Carolina 28655.

*CyberTip 2*

11. NCMEC received CyberTip #195424149 (CyberTip 2) from Facebook on June 20, 2024, at approximately 4:30PM (UTC). This tip also identified DEVINNEY as sending child pornography to Stamey via Facebook Messenger.

12. CyberTip 2 identified ten files that DEVINNEY sent to Stamey on June 17, 2024, at approximately 4:21PM (UTC), two of which depicted child pornography.

13. CyberTip 2 provided all the same account information regarding the Facebook Messenger accounts for DEVINNEY and Stamey that were provided in CyberTip 1, including the telephone numbers.

14. The two files identified as child pornography in CyberTip 2 depicted the following:

a. A video lasting approximately 30 seconds of a pubescent white female, approximately 12-14 years old, masturbating.

b. A video lasting approximately 44 seconds of a prepubescent white female, approximately 10-12 years old, exposing her vagina and breasts.

*Agents identify and interview DEVINNEY and Stamey*

15. The North Carolina State Bureau of Investigation (NCSBI) served an administrative subpoena on Charter Communications for account information associated with IP

address 75.143.188.107 in service on May 30, 2024, at approximately 10:58AM (UTC). Charter Communications responded with the following account information:

> Subscriber Name: Andrew DEVINNEY
> Service Address: 3695 Ridge Ct. Morganton, NC 28655-9170
> User Name or Features: andrew_devinney@charter.net, andrewdevinney@charter.net, andrewdevinney0811@charter.net, andrewdevinney94@gmail.com, and doofy_marine@charter.net.
> Account Number: 8315202290391189
> MAC: 2CEADCB11273
> Lease Log: Start Date: 07/01/2022 8:53PM / End Date: 07/20/2024 1:27PM

16. FBI agents located and interviewed DEVINNEY on August 13, 2024. During his interview, DEVINNEY explained that he and Stamey reside with one another, have two children together, and are engaged. DEVINNEY confirmed his and Stamey's Facebook account information and admitted to sending large amounts of pornography to Stamey, but claimed to be unsure whether he ever sent her child pornography. DEVINNEY also disclosed an old Facebook account under the name of "John Smith" that he claimed not to use anymore.

17. An FBI agent and a BCSO detective located and interviewed Stamey on August 26, 2024. Stamey admitted that DEVINNEY began sending her child pornography approximately a year prior. DEVINNEY transmitted almost all the child pornography material via Facebook Messenger. Stamey also admitted to using Reddit and Google to download child pornography and send it to DEVINNEY via Facebook Messenger. Stamey disclosed that DEVINNEY downloaded most of the child pornography from Kik and Reddit before sending it to her on Facebook Messenger. Stamey was unsure of the quantity of child pornography that she and DEVINNEY traded but affirmed that they had shared a large amount.

*Forensic analysis of DEVINNEY's cell phone*

18. FBI agents seized DEVINNEY's cell phone during his interview. Pursuant to a Federal search warrant, FBI performed a forensic analysis of DEVINNEY's cell phone and confirmed that it used the phone number 828-302-9582. Agents also recovered images depicting child pornography from the device. The forensic analysis revealed that DEVINNEY began using his cell phone to download and view child pornography at least as early as September 20, 2019, and confirmed that DEVINNEY used the cell phone to send child pornography to Stamey on July 12, July 29, and August 12, 2024. Agents also discovered that DEVINNEY had used his cellphone to send child pornography to his "John Smith" Facebook account on July 12, 2024.

19. The Facebook account User ID numbers for DEVINNEY's "Andrew Devinney" and "John Smith" accounts were found on DEVINNEY's cellphone during the forensic analysis:

a. "Andrew DeVinney" Account ID: #100010733371225

b. "John Smith" Account ID: #100052453491283

20. On August 5, 2024, the Burke County Sheriff's Office submitted a preservation request to Meta to preserve account information for the "Andrew DeVinney" Facebook account. On September 10, 2024, the FBI submitted a preservation request to Meta to preserve account information for the "John Smith" Facebook account.

## BACKGROUND CONCERNING FACEBOOK[4]

21. Meta owns and operates Facebook, a free-access social networking website that can be accessed at http://www.facebook.com. Facebook users can use their accounts to share

[4] The information in this section is based on information published by Meta on its Facebook website, including, but not limited to, the following webpages: "Privacy Policy," available at https://www.facebook.com/privacy/policy; "Terms of Service," available at https://www.facebook.com/legal/terms; "Help Center," available at https://www.facebook.com/help; and "Information for Law Enforcement Authorities," available at https://www.facebook.com/safety/groups/law/guidelines/.

communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

22. Meta asks Facebook users to provide basic contact and personal identifying information either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

23. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

24. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

25. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

26. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can "tag" other users in a photo or video, and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

27. Facebook users can use Facebook Messenger to communicate with other users via text, voice, video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

28. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

29. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or

content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

30. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

31. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

32. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

33. In addition to the applications described above, Meta provides users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

34. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user's IP address is retained by Meta along with a timestamp.

35. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables "Location History," "checks-in" to an event, or tags a post with a location.

36. Social networking providers like Meta typically retain additional information about their users' accounts, such as information about the length of service (including start date), the

types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

37. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In I's training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime

under investigation. Additionally, location information retained by Meta may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

38. Therefore, the servers of Meta are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

## INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## CONCLUSION

40. Based on the foregoing, I request that the Court issue the proposed search warrant.

41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the

requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

42. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

Respectfully,

*/s/ Jared Schaefer*
Jared Schaefer
Special Agent FBI

*This Affidavit has been reviewed by AUSA Alexis Solheim.*

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 12th day of September, 2024, at 3:03 PM EDT

W. Carleton Metcalf
United States Magistrate Judge

# ATTACHMENT A

## Property to Be Searched

This warrant applies to information associated with the following Facebook accounts that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California:

- Andrew DeVinney with associated user ID 100010733371225, and
- John Smith with associated user ID 100052453491283.

## ATTACHMENT B

### Particular Things to be Seized

**I. Information to be disclosed by Meta Platforms, Inc. ("Meta")**

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A for the time period of **July 1, 2023 – August 13, 2024**:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers;

future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, advertising ID, and user agent string;

(f) All other records and contents of communications and messages made or received by the user, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of Facebook searches performed by the account;

(i) The types of service utilized by the user;

(j) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(k) Records of any Facebook accounts that are linked to the account by machine cookies (meaning all Facebook user IDs that logged into Facebook by the same machine as the account); and

(l) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta is hereby ordered to disclose the above information to the government within 14 of issuance of this warrant.

## II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) (receipt and distribution of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of, knowing access, or attempted access with intent to view child pornography), involving ANDREW DEVINNEY since **July 1, 2023, to August 13, 2024**, including, for each user ID identified on Attachment A, information pertaining to the following matters:

a. Records related to "child pornography," as defined in 18 U.S.C. § 2256(8), and "child erotica," which means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

b. Records constituting evidence of or pertaining to an interest in child pornography or sexual activity with children;

c. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account owner;

d. Records showing or identifying the devices used to connect to the account; and

e. Records regarding the location of the user of the account during account activity and to help reveal the whereabouts of such person(s).

f. Evidence indicating the Account owner's state of mind as it relates to the crimes under investigation;

As used above, the term "records" includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage and any photographic form.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Meta Platforms, Inc. ("Meta"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Meta. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Meta, and they were made by Meta as a regular practice; and

b. such records were generated by Meta's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Meta in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Meta, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

| | |
|---|---|
| Date | Signature |